UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,158	07/25/2003	Adrian Patrick Kent	200206289-1	2520

22879 7590 01/26/2011

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
POPHAM, JEFFREY D	
ART UNIT	**PAPER NUMBER**
2491	

NOTIFICATION DATE	DELIVERY MODE
01/26/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ADRIAN PATRICK KENT, WILLIAM JOHN MUNRO,
TIMOTHY PAUL SPILLER, and RAYMOND G. BEAUSOLEIL

Appeal 2009-006596
Application 10/627,158[1]
Technology Center 2400

Before JOSEPH L. DIXON, JEAN R. HOMERE, and JAMES R. HUGHES, *Administrative Patent Judges*.

HOMERE, *Administrative Patent Judge*.

DECISION ON APPEAL[2]

---

[1] Filed on July 25, 2003. The real party in interest is Hewlett-Packard Development Co., LP. (App. Br. 2.)

[2] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

I. STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. §134(a) (2002) from the Examiner's final rejection of claims 1 through 49. (App. Br. 2.) We have jurisdiction under 35 U.S.C. § 6(b) (2008).

We reverse.

Appellants' Invention

Appellants invented a method for establishing a shared, secret, and random cryptographic key between a sender and a recipient utilizing a quantum communications channel. (Spec. 1, ll. 5-8.)

Illustrative Claim

Independent claim 1 illustrates the invention as follows:

> 1. A method of establishing a shared secret random cryptographic key between a sender and a recipient using a quantum communications channel, the method comprising:
>
> generating a plurality of random quantum states of a quantum entity, each random state being defied by a randomly selected one of a first plurality of bases in Hilbert space, the first plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space;
>
> transmitting the plurality of random quantum states of the quantum entity via the quantum channel to the recipient;
>
> measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a second plurality of bases in Hilbert space, the second plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space;
>
> transmitting to the recipient composition information describing a subset of the plurality of random quantum states;

analysing [sic] the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states;

establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar;

deriving, a first binary string and a second binary string, correlated to the first binary string, respectively from the transmitted and received plurality of quantum states not in the subset; and

carrying out a reconciliation of the second binary string to the first binary string by using error correction techniques to establish the shared secret random cryptographic key from the first and second binary strings.

Prior Art Relied Upon

The Examiner relies on the following prior art as evidence of unpatentability:

Franson	6,678,450	Jan. 13, 2004 (filed on Apr. 26, 1999)

Charles H. Bennett et al., "*Experimental Quantum Cryptography*," (Sept. 1991) (pgs. 1-28) (hereinafter "Bennett").

Denis Sych et al., "*Quantum cryptography with continuous alphabet*," (Apr. 2003) (M.V. Lomonosov Moscow State University, Russia) (on file with the International Laser Center and Faculty of Physics) (hereinafter "Sych").

Paul E. Black et al., "*Quantum Computing and Communication*," (Feb. 2002) (on file with the National Institute of Standards and Technology) (hereinafter "Black").

Rejections on Appeal

The Examiner rejects the claims on appeal as follows:

Claims 1 through 7, 10 through 13, 16 through 20, 22 through 24, 26 through 38, 41 through 43, and 46 through 49 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Bennett and Sych.

Claims 8, 9, 21, 25, 39, and 40 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Bennett, Sych, and Black.

Claims 14, 15, 44, and 45 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Bennett, Sych, and Franson.

Appellants' Contentions

Appellants contend that both Bennett and Sych disclose a reconciliation technique of identifying a string of qubits on which the recipient carried out measurements in a basis containing the qubit prepared by the sender. (App. Br. 9.) According to Appellants, Bennett discloses verifying that the photons in a subset are correctly measured utilizing basis reconciliation, utilizing the subset to determine a key, and discarding the rest. (*Id.* at 10-11.) Similarly, Appellants allege that Sych discloses a technique for basis reconciliation that may improve performance of quantum cryptography. (*Id.* at 11.) Appellants contend, however, that both Bennett and Sych fail to disclose deriving a statistical distribution from composition information describing a subset of transmitted random quantum states, and deriving a second statistical distribution from the composition information describing a subset of measured and received quantum states. (*Id.* at 10 & 11.) Appellants also argue that both Bennett and Sych fail to disclose analyzing the two sets of statistical distributions to verify whether the sets of

statistical distributions are sufficiently similar. (*Id.*) Additionally, Appellants allege that both Bennett and Sych fail to disclose deriving a first binary string from transmitted quantum states not in the earlier subset, and deriving a second binary string from received quantum states not in the earlier subset. (*Id.*)

Further, Appellants contend that Bennett's disclosure of Alice (i.e., the sender) and Bob (i.e., the receiver) communicating information pertaining to which measurements were made in the correct bases by Bob, and discarding those results that were measured with wrong bases, does not teach the claimed invention. (Reply Br. 2.) Appellants argue that the claimed invention does not have an underlying requirement of making known which photons had correctly measured bases and, subsequently, utilizing the correctly measured photons to generate a key. (*Id.* at 3.) Rather, Appellants allege that the claimed invention is directed to: 1) utilizing a subset of transmitted photons to derive statistical distributions describing transmitted and received quantum states; 2) discarding the subset; and 3) from the remaining quantum states, deriving a first binary string from the transmitted quantum states and a second binary string from the received quantum states. (*Id.*)

Examiner's Findings and Conclusions

The Examiner disagrees with Appellant's allegation that Bennett's data created from correctly measured photons becomes the key. (Ans. 18.) Rather, the Examiner finds that Bennett discloses performing additional processing after the base agreement communication. (*Id.* at 18-19.) In particular, the Examiner finds that Bennett discloses that two parties, Alice and Bob, communicate information regarding which measurements were

made in the correct bases by Bob, and discard the results there were measured with the wrong bases. (*Id.* at 19.) The Examiner finds that the parties compare polarizations of random subsets of photons in order to estimate an error rate and determine whether the data is sufficiently similar. (*Id.*) If there are no discrepancies found, the Examiner finds that the parties may safely conclude that there are few or no errors in the remaining un-compared data, and that little or none of the data is known to an eavesdropper. (*Id.*) Therefore, the Examiner finds that Bennett teaches or fairly suggests the "transmitting," "analyzing," and "establishing" steps, as recited in independent claim 1. (*Id.* at 19-20.)

Further, the Examiner finds that Bennett discloses Alice and Bob performing reconciliation based on the error correction to respective strings of bits, which includes partitioning the data into blocks of equal size and comparing the parity of each block. (*Id.* at 20.) If the parity matches, the Examiner finds that Bennett discloses tentatively accepting the blocks as correct, pending additional processing down the line. (*Id.*) If the parity does not match, the Examiner finds that Bennett discloses finding and correcting the errors. (*Id.*) Therefore, the Examiner finds that Bennett teaches deriving correlated binary strings and carrying out reconciliation of the bit strings by utilizing error correction techniques in order to establish a shared key from the bit strings. (*Id.*) Additionally, the Examiner finds that Bennett's disclosure in footnote 3, which includes comparing and sacrificing a small, random sample of bits in order to estimate the error rate, teaches that the data utilized in the reconciled bits includes data that is not included in the subset. (*Id.* at 20-21.)

Moreover, the Examiner finds that Sych discloses that the security condition is a condition ensuring that the amount of information that Bob receives from Alice exceeds the amount of information an eavesdropper receives from either Alice or Bob. (*Id.* at 21.) Therefore, the Examiner finds that Sych also teaches analyzing statistical distributions, establishing a level of confidence by verifying that the distributions are sufficient similar, discarding the data from the subset, and utilizing that data which was not in the subset to generate a key. (*Id.*)

II. ISSUE

Have Appellants shown that the Examiner erred in concluding that the combination of Bennett and Sych renders independent claims 1 unpatentable? In particular, the issue turns on whether the proffered combination teaches the following claim limitations:

(a) "transmitting to the recipient composition information describing a subset of the plurality of random quantum states," as recited independent claim 1; and

(b) "analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states," as recited in independent claim 1;

III. FINDINGS OF FACT

The following Findings of Fact (hereinafter "FF") are shown by a preponderance of the evidence.

Bennett

FF 1. Bennett discloses an apparatus and protocol to implement quantum key distribution, whereby two users exchange a random quantum transmission consisting of very faint flashes of polarized light, publicly discuss the sent and received version of these transmissions in order to estimate the extent of eavesdropping, and determine from the sent and received versions a small body of shared random information. (Abst.)

FF 2. Bennett discloses that basic quantum key distribution protocol begins with Alice sending a random sequence of the four canonical kinds of polarized photons to Bob. (4: ll. 37-38; *see also* fig. 1) Further, Bennett discloses that Bob measures the photons' polarization in a random sequence of bases. (*Id.* at ll. 39-41; *see also* fig. 1.) Additionally, Bob publicly announces the measurements he made and Alice publicly confirms whether such measurements were correct. (*Id.* at l. 41-5: l. 1; see also fig. 1.)

FF 3. Bennett discloses that Alice and Bob publicly agree to discard all bit positions from which Bob performed the wrong measurements. (5: ll. 1-2; *see also* fig. 1.) Similarly, Bennett discloses discarding bit positions where Bob's detectors failed to detect the photon. (*Id.* at 2-4; *see also* fig. 1.) Further, Bennett discloses interpreting the remaining data as a binary sequence according to the coding scheme. (*Id.* at ll. 6-8; *see also* fig. 1.)

FF 4. Bennett discloses that Alice and Bob test for eavesdropping by publicly comparing polarizations of a random subset of the photons on which they think they should agree. (*Id.* at ll. 11-13.) If no discrepancies are found, Bennett discloses that Alice and Bob safely conclude that there a few or no errors in the remaining un-compared data, and that little or none of it is known to an eavesdropper. (5: l. 18-6: l. 4.)

IV. ANALYSIS

Claim 1

Independent claim 1 recites, in relevant parts:

> 1) transmitting to the recipient composition information describing a subset of the plurality of random quantum states; 2) analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states.

As detailed in the Findings of Fact section above, Bennett discloses an apparatus and protocol for implementing quantum key distribution. (FF 1.) In particular, Bennett discloses that Alice sends a random sequence of four canonical kinds of polarized photons to Bob. (FF 2.) Further, Bennett discloses that Bob measures the photons' polarization in a random sequence of bases, Bob publicly announces the measurements to Alice, and Alice publicly confirms whether the measurements are correct. (*Id.*) Additionally, Bennett discloses that Alice and Bob publicly agree to discard all bit positions from which Bob performed the wrong measurements and where Bob's detectors failed to detect a photon. (FF 3.) Bennett discloses interpreting the remaining data as a binary sequence according to the coding scheme. (*Id.*) Next, Bennett discloses that Alice and Bob test for eavesdropping by publicly comparing the polarizations of a random subset of photons on which they should agree. (FF 4.) If no discrepancies are found, Bennett discloses that Alice and Bob can safely conclude that an eavesdropper did not corrupt the exchanged data. (*Id.*)

At best, we find that Bennett's disclosure of Alice and Bob publicly comparing the polarizations of the random subset of photons on which they should agree teaches that Alice transmits to Bob a random subset of photons for comparison. However, we find that Bennett's disclosure fails to teach or suggest that Alice transmits to Bob composition information describing a subset of the plurality of random quantum states, let alone analyzing both the received composite information and the measured quantum states corresponding to the subset in order to derive a first and second statistical distribution. While Bennett discloses that Alice transmits to Bob a random subset of photons for comparison, Bennett is silent in regards to whether the transmission includes composite information or metadata pertaining to the random subset of photons, such that the claimed steps of analyzing and deriving are capable of being completed without further transmissions or communications between Alice and Bob. Absent a showing that Bennett's quantum key distribution includes Alice transmitting to Bob composition information describing a subset of the plurality of random quantum states, and analyzing the received composition information and the measured quantum states corresponding to the subset in order to derive a first and second statistical distribution, we find that the Examiner improperly relied upon Bennett's disclosure to teach the disputed limitations. Further, we note that Sych fails to remedy the noted deficiencies in Bennett.

Since Appellants have shown at least one error in the rejection of independent claim 1, we need not reach the merits of Appellants' other arguments. It follows that Appellants have shown that the Examiner erred in concluding that the combination of Bennett and Sych renders independent claim 1 unpatentable.

Claims 2 through 49

Since independent claims 26 and 35, and dependent claims 2 through 25, 27 through 34, and 36 through 49, also recite at least one of the limitations discussed above, we find that Appellants have also shown error in the Examiner's rejection of these claims for the reasons set forth in our discussion of independent claim 1.

V. CONCLUSION OF LAW

Appellants have shown that the Examiner erred in rejecting claims 1 through 49 as being unpatentable under 35 U.S.C. § 103(a).

VI. DECISION

We reverse the Examiner's decision to reject claims 1 through 49 as being unpatentable under 35 U.S.C. § 103(a).

REVERSED

Vsh

HEWLETT-PACKARD COMPANY
INTELLECTUAL PROPERTY ADMINISTRATION
3404 E. HARMONY ROAD
MAIL STOP 35
FORT COLLINS, CO 80528